Software Product Description

PRODUCT NAME: Digital Authentication Server Version 1.0 **SPD 63.93.00**

In an open network computing environment, a workstation cannot be trusted to identify its users correctly to network services. In a distributed client/server environment your data is vulnerable. A client/server environment gives a large number of people access to valuable data. This data is more susceptible to fraud, hacking, sabotage and other security breaches.

To adequately protect a decentralized, widely distributed environment, products that combine various protocols and techniques based on advanced encryption, multiple level of password protection, and other schemes are required.

DESCRIPTION

Digital Authentication Server provides network authentication service to user, servers and client programs based on the Kerberos™ protocol. It uses DES encryption to do private key encryption of service keys, ensuring that entities are authentic. All of this is managed centrally with client/server tools, so the system administrator can manage the entire security environment from any UNIX® machine.

By centralizing the security mechanism, only the security server need be in a physically secure area. Access to individual workstation is no longer a security issue.

The Kerberos V5 standard, developed at the Massachusetts Institute of Technology, provides trusted third-party authentication service. Principals involved in a transaction trust Kerberos (the "trusted third party") to verify that both sides are who they claim to be. Users, for example, must prove their identity for each desired Kerberized service. The server must also prove its identity to the client requesting a Kerberized service. The authentication requirement of both parties removes the need for each client machine on the network to be physically secure, because the party being authenticated is the user and not the machine. With Kerberos V5, client/server software programs are prevented from masquerading as servers, and users are prevented from impersonating one another.

Each time an entity authenticates with Kerberos (for example, when a user logs in) the Kerberos server issues an initial ticket-granting ticket. This initial ticket contains the information necessary to prove the identity of the user and is used when the user requests additional tickets from other services. The login process is where this typically occurs, but Kerberos authentication can take place between nonhuman clients, such as between master Kerberos server and its slave Kerberos servers.

As a system administration tool, Digital Authentication Server offers centralized management of user passwords. It eliminates the passing of clear-text passwords over the wire and the need for trusted host systems. The Kerberos development environment enables the creation of network-secure client/server applications.

Digital Authentication Server includes a complete, well-documented development environment for Kerberos V5 and GSSAPI on both UNIX and PC machines.

The Generic Security Service Application Program Interface (GSSAPI) provides security to applications in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments, such as Kerberos, DCE security, and public key systems.

Digital Authentication Server includes:

- Master server
- Admin facility
- Slave server(s)
- Password Management tools:
  - Minimum Length
  - Dictionary
  - Expiration
  - Re-Use Prevention
- User and Admin tools
- Development Libraries

- Kerberized r-commands
- Documented programmers guide

The Digital Authentication Server product includes:

Server Side:

Kerberos database server

The information necessary to perform authentication such as principals and passwords is stored in the Kerberos master database, which resides on the Kerberos master server host.

kadmind

Provides an interface for performing administration functions on the Kerberos master database over the network.

kprop (On slave)

Propagates Kerberos database from master Kerberos server to slave server.

kpropd (On slave)

Receives Kerberos database on slave from master Kerberos server

kdb5_edit

Edits Kerberos database. Can only be run on Kerberos master server

Kerberos database management utilities

Client Side:

kinit

Creates a new TGT. Use this command if your TGT expires.

klist

Lists the tickets you currently hold. Use this command to check your expiration times.

kdestroy

Destroys the ticket you currently hold. Use this command to insure security.

kpasswd

Changes your Kerberos password.

ksu

Kerberized su program.

kaddsrvkey

Installs server principals into keytab.

kadmin Utility

For remote administration of database.

Kerberized telnet

Kerberized r-commands

The Kerberized r-commands,*rlogin, rcp, rsh*, allow remote system access in a controlled, secure manner.

tkoffice

GUI user interface.

Development Libraries:

With krb5 and GSSAPI interfaces.

Documentation set includes:

- Hardcopy guides, a user reference card, UNIX man pages, and PC Window help.
- Digital Authentication Server System Administrator's Guide
- Digital Authentication Server Application Programmer's Interface Guide
- Digital Authentication Server Installation Guide
- Digital Authentication Server User's Guide

HARDWARE REQUIREMENTS

See sections that list servers and clients supported. Minimum hardware requirement depends on environment and configuration.

Disk Space Requirements

35MB - binaries and libraries 10MB - minimum for Kerberos database

This count refers to the disk space required on the system disk where appropriate. The size is approximate; actual sizes may vary depending on the user's system environment, configuration, and software options.

For more information on the recommended system size for use of Digital Authentication Server contact your local Digital office.

SOFTWARE REQUIREMENTS

Server Platforms (master/slave):

- Digital UNIX V3.0-V3.2
- HP-UX® V9.03
- Solaris® V2.3

Client Platforms:

- Digital UNIX V3.0-V3.2
- HP-UX V9.03

- Solaris V2.3
- SunOS™ V4.1.4
- MS Windows™ V3.1

GROWTH CONSIDERATIONS

The minimum hardware/software requirements for any future version of this product may be different from the requirements for the current version.

DISTRIBUTION MEDIA

CD–ROM for UNIX platforms. RX23 floppy diskettes for MS Windows.

ORDERING INFORMATION

Software Licenses:

QL–3QNA*–**	Digital Authentication Server Digital UNIX Traditional Server License
QL–3QPA*–**	Digital Authentication Server HP-UX Traditional Server License
QL–3QQA*–**	Digital Authentication Server Solaris Traditional Server License
QL–3QSA*–**	Digital Authentication Server UNIX Workstation Concurrent Client License
QL–3QTA*–**	Digital Authentication Server MS Windows Concurrent Client License

Software Media:

QA–3QNAA–H8	Software Media Digital UNIX
QA–3QPAA–H8	Software Media HP-UX
QA–3QQAA–H8	Software Media Solaris
QA–3QSAA–H8	Software Media SunOS
QA–3QTAA–HC	Software Media Client MS Windows

Software Documentation:

QL–3QNAA–GZ	Software Documentation ALL Platforms

Software Product Services:

* QT–3QNA*–**

* QT–3QPA*–**

* QT–3QQA*–**

* QT–3QSA*–**

* QT–3QTA*–**

* Denotes variant fields. For additional information on available licenses, services, and media, refer to the appropriate price book.

The above information is valid at time of release. Please contact your local Digital office for the most up-to-date information.

SOFTWARE LICENSING

This software is furnished only under a license. For more information about Digital's licensing terms and policies, contact your local Digital office.

SOFTWARE PRODUCT SERVICES

A variety of service options are available from Digital. For more information, contact your local Digital office.

SOFTWARE WARRANTY

Warranty for this software product is provided by Digital with the purchase of a license for the product as defined in the Software Warranty Addendum of this SPD.